



MULTI-DWELLING UNIT DEPLOYMENT GUIDE



Reservation of Rights

Cambium reserves the right to make changes to any products described herein to improve reliability, function, or design, and reserves the right to revise this document and to make changes from time to time in content hereof with no obligation to notify any person of revisions or changes. Cambium recommends reviewing the Cambium Networks website for the latest changes and updates to products. Cambium does not assume any liability arising out of the application or use of any product, software, or circuit described herein; neither does it convey license under its patent rights or the rights of others. It is possible that this publication may contain references to, or information about Cambium products (machines and programs), programming, or services that are not announced in your country. Such references or information must not be construed to mean that Cambium intends to announce such Cambium products, programming, or services in your country.

Copyrights

This document, Cambium products, and 3rd Party software products described in this document may include or describe copyrighted Cambium and other 3rd Party supplied computer programs stored in semiconductor memories or other media. Laws in the United States and other countries preserve for Cambium, its licensors, and other 3rd Party supplied software certain exclusive rights for copyrighted material, including the exclusive right to copy, reproduce in any form, distribute and make derivative works of the copyrighted material. Accordingly, any copyrighted material of Cambium, its licensors, or the 3rd Party software supplied material contained in the Cambium products described in this document may not be copied, reproduced, reverse engineered, distributed, merged or modified in any manner without the express written permission of Cambium. Furthermore, the purchase of Cambium products shall not be deemed to grant either directly or by implication, estoppel, or otherwise, any license under the copyrights, patents or patent applications of Cambium or other 3rd Party supplied software, except for the normal non-exclusive, royalty free license to use that arises by operation of law in the sale of a product.

Restrictions

Software and documentation are copyrighted materials. Making unauthorized copies is prohibited by law. No part of the software or documentation may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, without prior written permission of Cambium.

License Agreements

The software described in this document is the property of Cambium and its licensors. It is furnished by express license agreement only and may be used only in accordance with the terms of such an agreement.

High Risk Materials

Cambium and its supplier(s) specifically disclaim any express or implied warranty of fitness for any high-risk activities or uses of its products including, but not limited to, the operation of nuclear facilities, aircraft navigation or aircraft communication systems, air traffic control, life support, or weapons systems (“High Risk Use”).

This product is not restricted in the EU. Any High Risk is unauthorized, is made at your own risk and you shall be responsible for any and all losses, damage or claims arising out of any High-Risk Use.

Contents

- Contents** **3**
- Introduction** **5**
- Planning and Pre-Configuration** **6**
 - Locations 6
 - Residents 6
 - Accessibility 6
 - Security 7
 - Guests 7
 - Building and Construction Materials 7
 - Challenges 7
- Best Practices/Design Recommendations** **8**
 - AP Selection 8
 - AP Mounting Location Precautions 8
 - AP Orientation 8
- Configuration Best Practices- WLANs and AP Groups** **9**
 - WLAN Configuration 9
 - AP Group Configuration 9
 - Radio configuration (General settings) 9
 - 2.4GHz Radio 10
 - 5GHz Radio 13
 - 6GHz Radio 17
 - Validation 20
- User-Defined Overrides** **21**
- ePSKs** **24**
 - General benefits of ePSKs 24
 - Dynamic VLAN's 24
 - ePSK Creation / Configuration 24
 - Import/Export and Delete 26

AAA Vendors already integrated	27
ePSK Configuration	28
cnMaestro Configuration - Proxy through controller	28
Personal Wi-Fi Network	30
Benefits of Personal Wi-Fi Network	30
Personal Wi-Fi Network configuration	30
Troubleshooting	31
Show Commands	31
Enable debug logging from AP CLI - to view the ePSK cache entries on the system	31
Remote debugging from cnMaestro	31
Debugging	32
Summary	33
Cambium Networks	34

Introduction

Multi-dwelling units (MDUs) include apartments, condominiums, assisted living facilities, dormitories, hotels/motels, multi-floor buildings, and any other environment where multiple separate housing or residential units are contained within one building or multiple buildings within a complex of buildings.

High-performing Wi-Fi with easy access is expected by the residents and must be provided as an amenity for complexes to compete. MDUs vary in type and size, and there are some variations in best practices between the different MDU types, but the basic design remains the same.

Managed Wi-Fi is a big win for residents as they do not have to deal with service providers such as Spectrum or Time Warner. A cleaner spectrum is another benefit as the management will not have to design a Wi-Fi network around every resident's Wi-Fi router, which will choose radio channels and power settings at random and cause havoc to the house Wi-Fi.

Managed Wi-Fi is beneficial to property management as they have numerous types of IoT devices such as access control, temperature regulation, and lighting, that require internet connectivity, and Wi-Fi is another source of revenue.

With managed Wi-Fi, it is still possible for a tenant to have a private network in their living quarters and public Wi-Fi provided in the common areas.

Cambium Networks provides high-performance wireless solutions that support MDUs in any configuration or size. This document describes Cambium Networks Enterprise Access Points and cnMaestro management solutions that are best deployed in MDU environments and describes best practices for designing and deploying Wi-Fi networks for optimal results.

Planning and Pre-Configuration

An MDU is comprised of different Wi-Fi zones, where each zone has a different set of client devices, use cases, and a different RF interference profile.

Consider how these zones impact the AP Group configuration:

Locations

1. Apartments
 - People who live here, stream TV to Apple TV, Roku, Firestick, etc.
 - A mix of very old and new devices.
 - Some personal IoT devices.
2. Common indoor areas such as laundry and exercise rooms
 - People spend as little time as necessary here, however, they like to be entertained here.
 - Personal devices are most likely to be a smartphone and a tablet.
 - Facilities IoT devices.
3. Common outdoor areas such as the pool area and tennis courts
 - People come here to do something specific and may not always want to bring their network.
 - Poolside where they want to stream music.
 - Tennis courts can require longer-range devices.

Now consider these aspects of different Wi-Fi network requirements:

Residents

In an MDU network, the residents are the most important entity. They always have the option of deploying their own Wi-Fi. The problem with this is, especially in the denser deployments, that when residents start to implement their solutions, there tend to be more problems with interference. If you provide poor Wi-Fi for the residents, they will be forced to add their own. That will, in turn, make Wi-Fi even worse for everyone. It is in your best interest, and that of the residents, to provide excellent Wi-Fi to everyone.

Accessibility

Access to the Wi-Fi network must be easy: easy to find, easy to connect, and easy to use. This includes all devices that residents use. That list is much longer than ever before with not only PCs and laptops, but also printers, TVs, Apple TV, Xbox, PlayStation Roku, Alexa, tablets, iPods, smart watches, refrigerators, thermostats, and surveillance cameras. Some of these devices utilize broadcast protocols such as Bonjour and CUPS to advertise their services.

In this type of environment, you will not enable Client Isolation as you would for a guest network.

Security

Each residential unit must be segmented from other users of the network. However, there is a real need to allow all devices within a residence to have free communication between them. Each residence needs to be treated as a unique and separate network. It is also important to prevent unauthorized users from accessing the network as they could take up bandwidth intended for the residents. Apart from this, the common areas of the MDUs will have Wi-Fi network availability where users can connect without worrying about security since each user is in a separate VLAN.

Guests

The choice to allow guest access should be considered, along with an implementation of how to limit that access to valid guest users and not just someone living or loitering close by. It is also important to limit guest access so that it does not impact bandwidth reserved for residents.

Building and Construction Materials

Typical building construction materials include wood studs and drywall for interior walls and a double layer of drywall on each side for common walls shared between apartments. (Drywall typically reduces the signal strength by 3dbm.)

A layer of 'lightweight' concrete is typically poured between floors. (ie. Between the second and third floors, between the third floor and fourth floors, etc.). This attenuates the signals between floors.

While these construction materials attenuate signals to some degree, the signals still pass through these materials and can cause interference for neighboring networks.

Challenges

Due to the sheer number of access points in a single building, co-channel interference is a major concern. Proper deployment of APs and radio configurations is required to optimize the balance between a signal that is strong enough to provide good throughput versus a signal that is so strong as to cause interference with other nearby radios.

There will be overlapping cells, so channels and power are very important, especially in the 2.4GHz band and channel separation in the 5GHz band to avoid adjacent channel interference.

Best Practices/Design Recommendations

Cambium APs are not “one size fits all”. APs are designed for optimal performance in different areas. You must select the correct AP for the type of environment it will be deployed in. The wall-mounted XV2-22H or XV2 access points will work best in the residences, whereas the XE3 or XE5 will work best in higher-density / higher-capacity environments.

AP Selection

XV2-22H - Low profile, wall plate Wi-Fi 6 access point. Designed for apartments, hotel rooms, and dormitories.

XV2-2X - two radios, Wi-Fi 6 access point designed for low to medium numbers of simultaneous clients with high-capacity usage.

XV2-21X - 2 radios, Wi-Fi 6 access point designed for low numbers of simultaneous clients with low-capacity usage.

XV2-23T - 2 radios, Wi-Fi 6 outdoor access point with omnidirectional antennas. Designed for low to medium coverage, client counts, and capacity.

XE3-4 - Three radios, Wi-Fi 6E access point with SDR. Designed for high-density and high-capacity environments.

XE5-8 - Five radios, Wi-Fi 6E access points with 2 SDRs. Designed for high-density and high-capacity environments.

AP Mounting Location Precautions

- Mount APs in central areas.
- Avoid placing AP near exterior walls where the signal is “wasted” by providing coverage outside the residence.
- Avoid placing AP behind obstacles such as A/C ducts and vents.

AP Orientation

Mount APs on a ceiling, in a horizontal position.

Configuration Best Practices- WLANs and AP Groups



Note

All Wireless/Wired configurations can be default or Network-specific except the below feature configurations.

WLAN Configuration

1. **UAPSD:** Enabling UAPSD might result in lower throughput hence it should be disabled. However, in case of extensive roaming scenarios/open hall deployment, UAPSD should be enabled.
2. **Band Steering:** When WLAN is mapped to the dual-band, set Band Steering to **Low**. This will help to steer clients to the 5GHz radio during client association. Associating too many clients on the 2.4 GHz band can result in channel congestion. Setting the aggressiveness to “Low” will help 2.4GHz sticky clients associate with the 5GHz radio by not responding to the first few 2.4GHz association requests. Configuring this setting to “**Normal**” or “**Aggressive**” can result in client disconnection while roaming between radios of the same AP.
3. **Fast Roaming Protocol (.11r):** This should be **Enabled** in MDU deployment common areas as it can help while clients are roaming between APs.
4. **PMF (.11w):** This can be **disabled** as it is not mandatory for security types such as open and WPA2. It should be set to **Mandatory** only while WPA3 security is configured.
5. **Fast Roaming Protocol (.11k / .11v):** This can be disabled for MDU residences as it can trigger roaming. However, you should enable these protocols in radios that are in common areas.

AP Group Configuration



Note

All Wireless/Wired configurations can be default or Network-specific except the below configurations.

Radio configuration (General settings)

- Disable lower data rates for management frames only which provides for smaller coverage cells by disregarding clients with very low signal strength and low data rates. This will improve throughput for individual clients and will also benefit all other clients connected to the radio by eliminating the slower data rates that use more time on a channel. These low data rates could be due to distance from AP and other obstacles.
- 20MHz channel
- Low power settings
- Keep minimum unicast rate at default

2.4GHz Radio



Note

In many cases, there will be more than three 2.4GHz radios within range of each other which will lead to co-channel interference due to only having 3 channels to operate on. In this case, you will need to decide to either lower the power on the 2.4GHz radios or disable the 2.4GHz radios that are causing the interference.

1. **Channels:** Select non-overlapping channels. Use only channels 1, 6, or 11.
2. **Transmit Power:** Use the access point's Wi-Fi Analyzer under Tools to check the power on nearby Cambium AP radios before deciding this value. Ideally, you will set the transmit power to "Auto" and let the system determine the power setting so that the optimal cell overlap is achieved.

Figure 1: 2.4GHz radio Transmit Power configuration

2.4 GHz Band | 5 GHz Band | 6 GHz Band

Basic

Status

Enabled Disabled Enable/Disable operation of this radio

Channel

Auto Only 'Auto' value is allowed. Configure static channel under the 'Advanced Settings' section available on the Access Point level configuration page [Learn more](#)

Candidates Channel

Specific Space separated list of channels

Candidate channels is a list of channels on which AP can operate. List of channels depend on the band and country.

Channel Width

20 Operating width of the channel

Transmit Power

Auto Radio transmit power in dBm (4 to 30; subject to regulatory limit)

Beacon Interval

100 Beacon interval in ms (50 to 3500) ⓘ

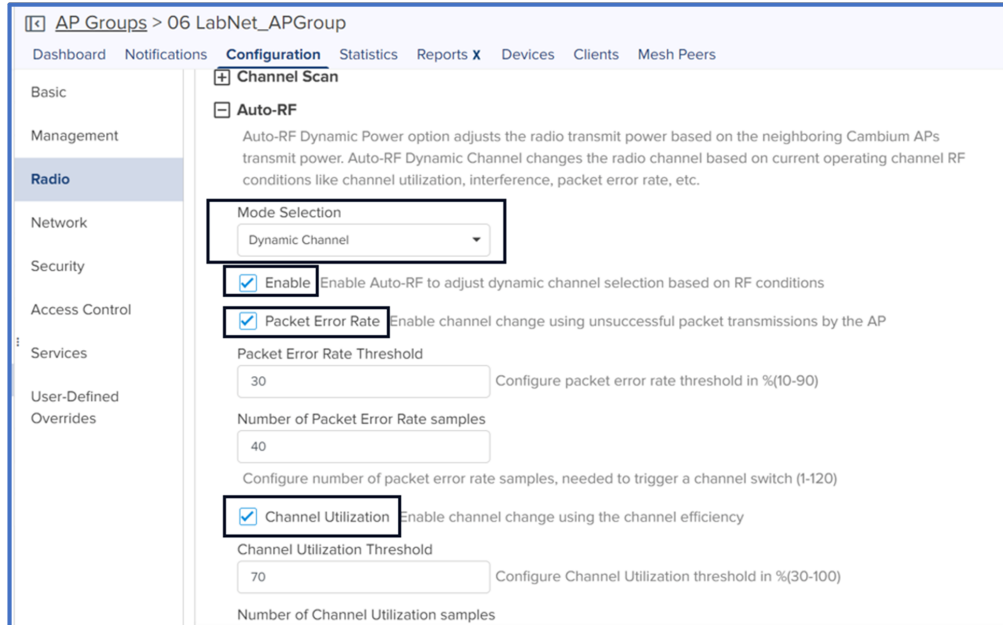
Minimum Unicast Rate

1 Configure the minimum unicast management rate (Mbps)

3. **Auto-RF Dynamic Channel :** This helps to change channels dynamically based on RF factors. See the below figures to enable and configure Dynamic Channel.

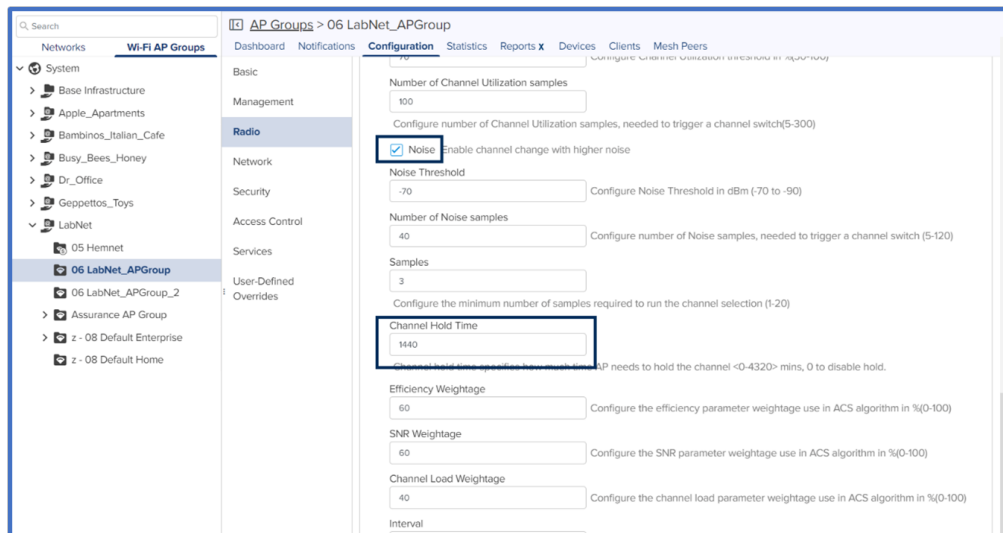
Configure Dynamic Channel as follows:

- a. Select Dynamic Channel as the Mode Selection
- b. Enable Auto-RF
- c. Enable Packet Error Rate
- d. Enable Channel Utilization. Use the default threshold configurations.

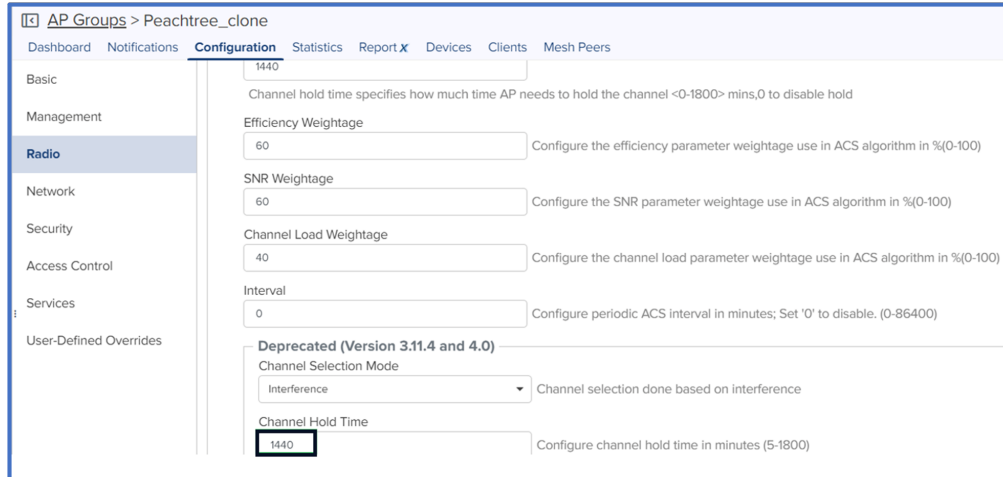


e. Enable Noise

f. Set Channel Hold Time to 1440



g. Under the **Deprecated** version of cnMaestro (Version 3.11.4 and 4.0) configure **Channel Hold Time** to 1440.



4. **Auto-RF Dynamic Power** – This helps to assign power levels dynamically based on RF factors. See the below figures to enable and configure Dynamic Power.



Note

Determine the values for the below two parameters (minimum transmit power and overlapping threshold), based on overlapping signals between Cambium neighboring devices. Use the Wifi Analyzer under cnMaestro Tools to check the nearby signal strength from other Cambium devices before deciding this value.

For example, if the Wi-Fi Analyzer shows you a neighboring Cambium device with an SNR of -35, then it means there will be a 100% overlap for that ssid/wlan.

Using the table below, you can reduce the required overlap threshold from 100% to the required value based on your needs. In the case where you see weak signals in areas within the residence, revisit these values after evaluating the network performance for a few days.

Table 1: Cell size overlap threshold mapping to a Pre-Derived RSSI value

Configured “auto-rf dynamic-power cellsize-overlap-threshold” on DUT (Cli: “auto-rf dynamic-power cellsize-overlap-threshold”)	RSSI observed on Neighbor APs (“show wireless neighbors autoce11”) (execute on neighbor AP)
0%	-90 (-85 to -95)
10%	-87 (-80 to -95)
20%	-84 (-80 to -90)
30%	-81 (-75 to -90)
40%	-78 (-70 to -85)
50%	-75 (-70 to -80)
60%	-72 (-65 to -80)
70%	-69 (-65 to -75)

Configured “auto-rf dynamic-power cellsize-overlap-threshold” on DUT (Cli: “auto-rf dynamic-power cellsize-overlap-threshold”)	RSSI observed on Neighbor APs (“show wireless neighbors autocell”) (execute on neighbor AP)
80%	-66 (-60 to -70)
90%	-63 (-55 to -70)
100%	-60 (-55 to -65) (SNR 35)

Configure Dynamic Power as follows:

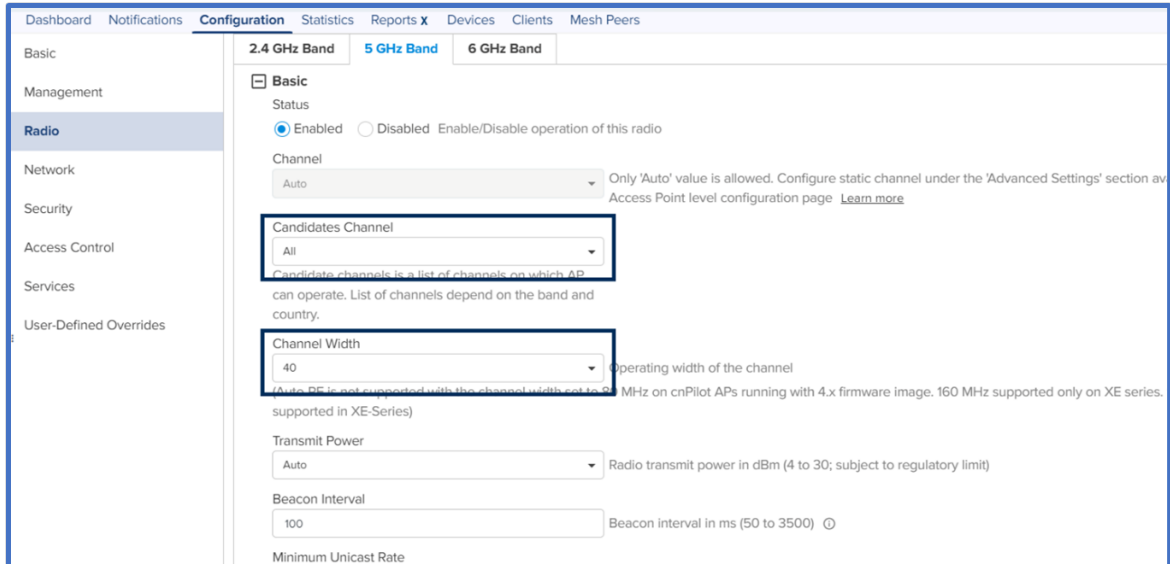
- a. Select Dynamic Power as the Mode Selection
- b. Enable Dynamic Power
- c. Select By-Band
- d. Set Minimum Neighbor Threshold to 1

The screenshot shows the configuration page for Auto-RF. The left sidebar contains a navigation menu with items: Radio, Network, Security, Access Control, Services, and User-Defined Overrides. The main content area is titled "Auto-RF" and includes the following settings:

- Mode Selection:** A dropdown menu set to "Dynamic Power".
- Enable:** A checked checkbox labeled "Enable Dynamic Power management".
- By-Band:** A radio button selected, labeled "By-Band Set dynamic power mode by-channel / by-band".
- Minimum Transmit Power:** A text input field set to "10".
- Minimum Neighbour Threshold:** A text input field set to "1".
- Cellsize Overlap Threshold:** A text input field set to "50".

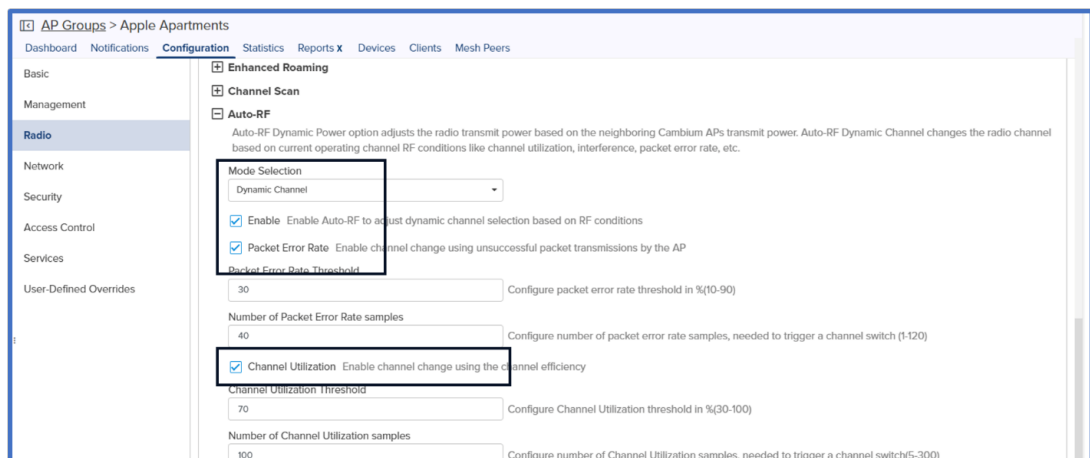
5GHz Radio

1. **Channels:** Under **Candidates Channel**, select **All**.
2. **Channel Width:** Set the **Channel Width** to 40 MHz.

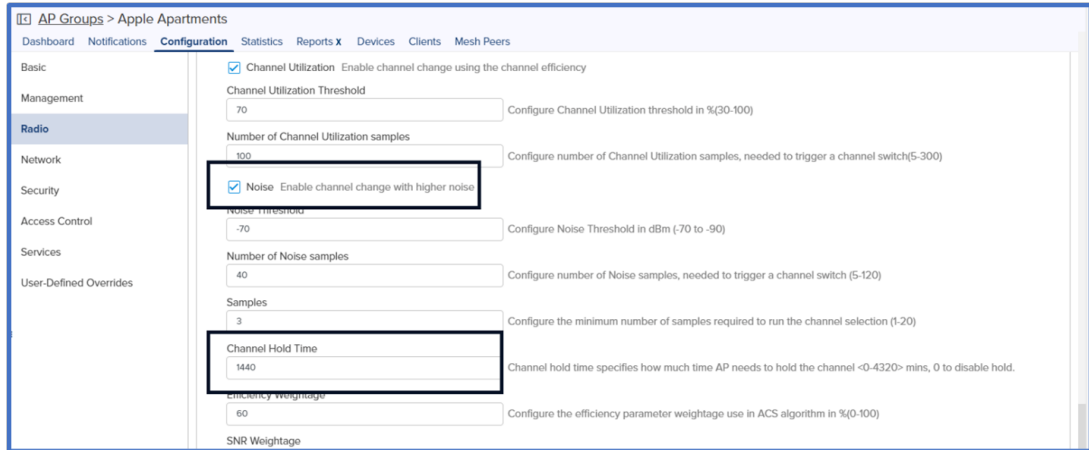


3. **Auto-RF Dynamic Channel:** This helps to change channels dynamically based on RF conditions. Enable the below checkboxes and change highlighted values.

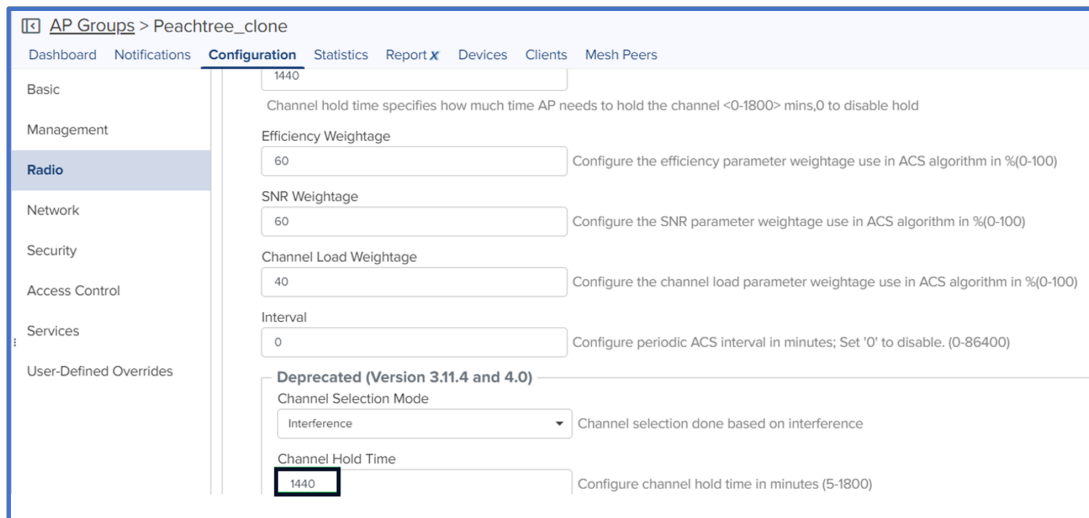
- a. Select Dynamic Channel as the Mode Selection
- b. Enable Auto-RF
- c. Enable Packet Error Rate
- d. Enable Channel Utilization. Use the default threshold configurations.



- e. Enable Noise
- f. Set Channel Hold Time to 1440



- g. Under the **Deprecated** version of cnMaestro (Version 3.11.4 and 4.0) configure **Channel Hold Time** to 1440.



5. Auto-RF Dynamic Power – This helps to assign power levels dynamically based on RF conditions. See the below figures to enable and configure Dynamic Power.



Note

Determine the values for the below two parameters (minimum transmit power and overlapping threshold), based on overlapping signals between Cambium neighboring devices. Use the Wifi Analyzer under cnMaestro Tools to check the nearby signal strength from other Cambium devices before deciding this value.

For example, if the Wi-Fi Analyzer shows you a neighboring Cambium device with an SNR of -35, then it means there will be a 100% overlap for that ssid/wlan. Using the table below, you can reduce the required overlap threshold from 100% to the required value based on your needs. In the case where you see weak signals in areas within the residence, revisit these values after evaluating the network performance for a few days.

Table 2: Cell size overlap threshold mapping to a Pre-Derived RSSI value

Configured “auto-rf dynamic-power cellsize-overlap-threshold” on DUT (Cli: “auto-rf dynamic-power cellsize-overlap-threshold”)	RSSI observed on Neighbor APs (“show wireless neighbors autocell1”) (execute on neighbor AP)
0%	-90 (-85 to -95)
10%	-87 (-80 to -95)
20%	-84 (-80 to -90)
30%	-81 (-75 to -90)
40%	-78 (-70 to -85)
50%	-75 (-70 to -80)
60%	-72 (-65 to -80)
70%	-69 (-65 to -75)
80%	-66 (-60 to -70)
90%	-63 (-55 to -70)
100%	-60 (-55 to -65) (SNR 35)

Configure Dynamic Power as follows:

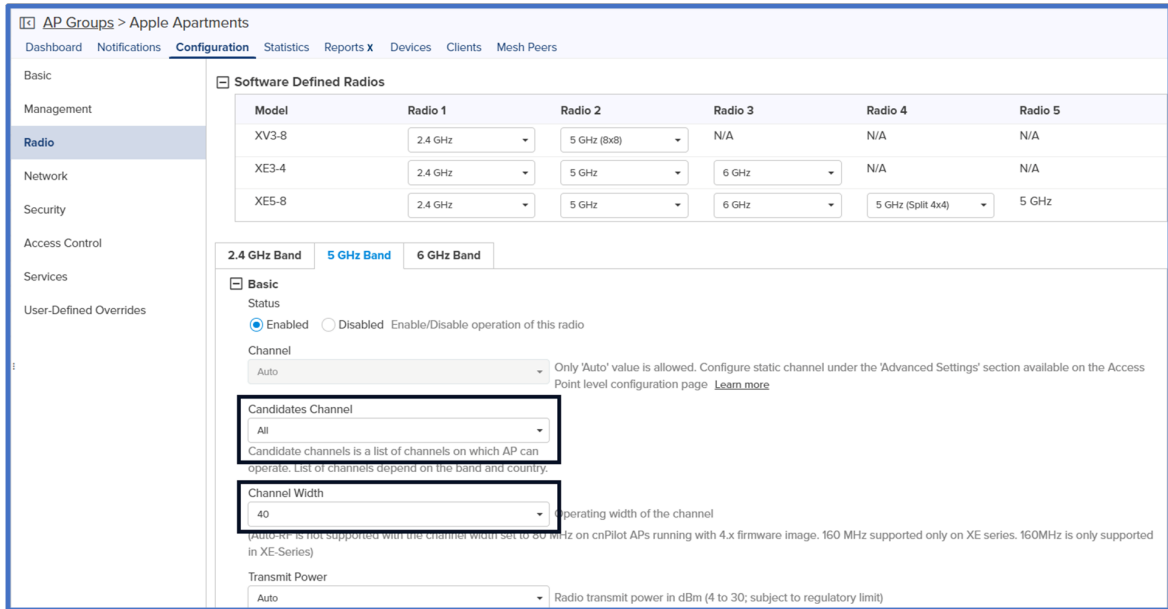
- a. Select **Dynamic Power** as the Mode Selection
- b. **Enable** Dynamic Power
- c. Select **By-Band**
- d. **Minimum Neighbour Threshold - 1**

The screenshot shows the configuration page for a radio interface. On the left is a navigation menu with categories: Radio, Network, Security, Access Control, Services, and User-Defined Overrides. The main content area is titled 'Radio' and contains several settings:

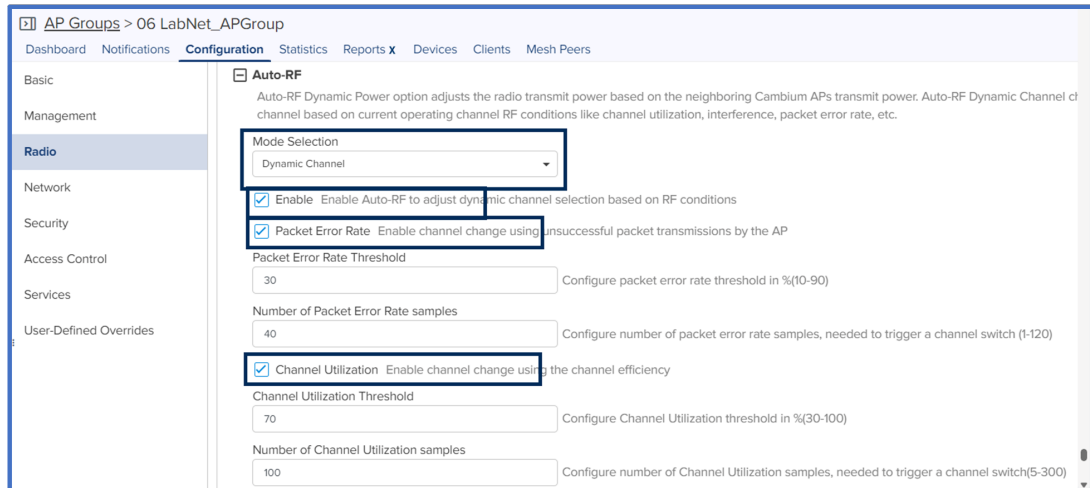
- Dwell Rest Time:** 25 (Configure dwell split time to spend on foreign channel)
- Dwell Rest Time:** 100 (Configure time interval between scans on same channel (100-1000))
- Channel Switch Announcement:** Use channel switch announcement as a part of channel change
- Auto-RF:**
 - Auto-RF Dynamic Power option adjusts the radio transmit power based on the neighboring Cambium APs transmit power. Auto-RF Dynamic Channel based on current operating channel RF conditions like channel utilization, interference, packet error rate, etc.
 - Mode Selection:** Dynamic Power
 - Enable:** Enable Dynamic Power management
 - By-Channel
 - By-Band:** Set dynamic power mode by-channel / by-band
 - Minimum Transmit Power:** 10 (Minimum transmit power that the AP can assign to a radio when adjusting automatic cell sizes (0-100))
 - Minimum Neighbour Threshold:** 1 (The Minimum number of neighbors to consider for power reduction by autocell logic. (1-10))
 - Cellsize Overlap Threshold:** 50 (Cell overlap that will be allowed when the AP is determining automatic cell sizes (0-100))

6GHz Radio

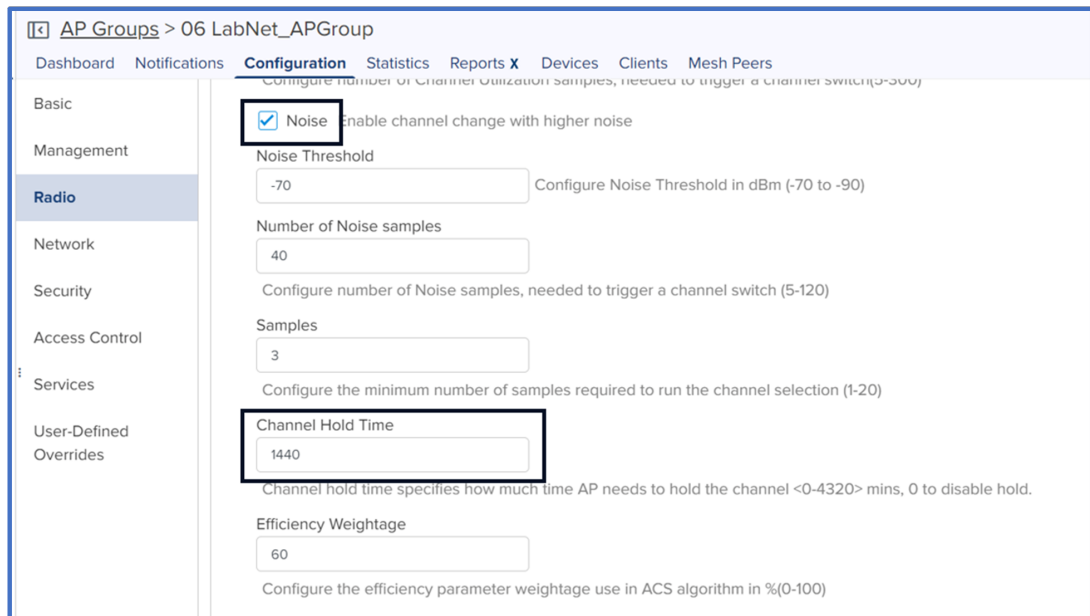
1. **Channels:** Under **Candidates Channel**, select **All**.
2. Set **Channel Width** to **40 MHz**



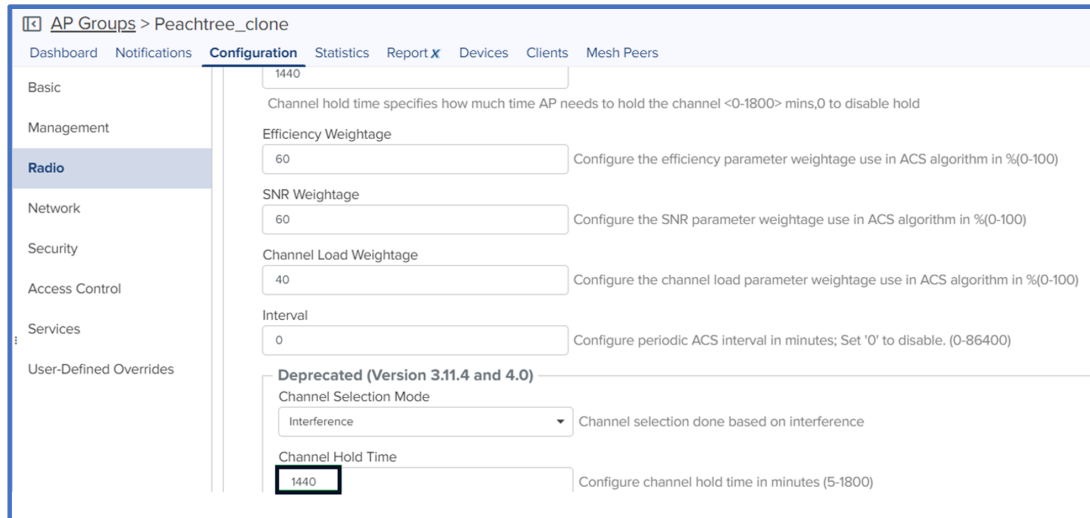
3. **Auto-RF Dynamic Channel:** This helps to change channels dynamically based on RF conditions. Enable the below checkboxes and change highlighted values.
 - a. Select Dynamic Channel as the Mode Selection
 - b. Enable Auto-RF
 - c. Enable Packet Error Rate
 - d. Enable Channel Utilization. Use the default threshold configurations.



- e. Enable **Noise**. Use the default threshold configurations. Configure **Channel Hold Time** to 1440.



- f. Under the **Deprecated** version of cnMaestro (Version 3.11.4 and 4.0) configure **Channel Hold Time** to 1440.



6. **Auto-RF Dynamic Power** – This helps to assign power levels dynamically based on RF conditions. See the below figures to enable and configure Dynamic Power.



Note
 Determine the values for the below two parameters (minimum transmit power and overlapping threshold), based on overlapping signals between Cambium neighboring devices. Use the Wifi Analyzer under cnMaestro Tools to check the nearby signal strength from other Cambium devices before deciding this value.

For example, if the Wi-Fi Analyzer shows you a neighboring Cambium device with an SNR of -35, then it means there will be a 100% overlap for that ssid/wlan. Using the table below, you can reduce the required overlap threshold from 100% to the required value based on your needs. In the case where you see weak signals in areas within the residence, revisit these values after evaluating the network performance for a few days.

Table 3: Cell size overlap threshold mapping to a Pre-Derived RSSI value

Configured “auto-rf dynamic-power cellsize-overlap-threshold” on DUT (Cli: “auto-rf dynamic-power cellsize-overlap-threshold”)	RSSI observed on Neighbor APs (“show wireless neighbors autoocell”) (execute on neighbor AP)
0%	-90 (-85 to -95)
10%	-87 (-80 to -95)
20%	-84 (-80 to -90)
30%	-81 (-75 to -90)
40%	-78 (-70 to -85)
50%	-75 (-70 to -80)
60%	-72 (-65 to -80)
70%	-69 (-65 to -75)

Configured “auto-rf dynamic-power cellsize-overlap-threshold” on DUT (Cli: “auto-rf dynamic-power cellsize-overlap-threshold”)	RSSI observed on Neighbor APs (“show wireless neighbors autocell”) (execute on neighbor AP)
80%	-66 (-60 to -70)
90%	-63 (-55 to -70)
100%	-60 (-55 to -65) (SNR 35)

Configure Dynamic Power as follows:

- Select **Dynamic Power** as the Mode Selection
- Enable** Dynamic Power
- Select **By-Band**
- Set **Minimum Neighbor Threshold** to 1

The screenshot shows the configuration page for a radio. The 'Auto-RF' section is expanded, showing the following settings:

- Mode Selection:** Dynamic Power
- Enable** Enable Dynamic Power management
- By-Channel
- By-Band** Set dynamic power mode by-channel / by-band
- Minimum Transmit Power:** 10
- Minimum Neighbour Threshold:** 1
- CellSize Overlap Threshold:** 50

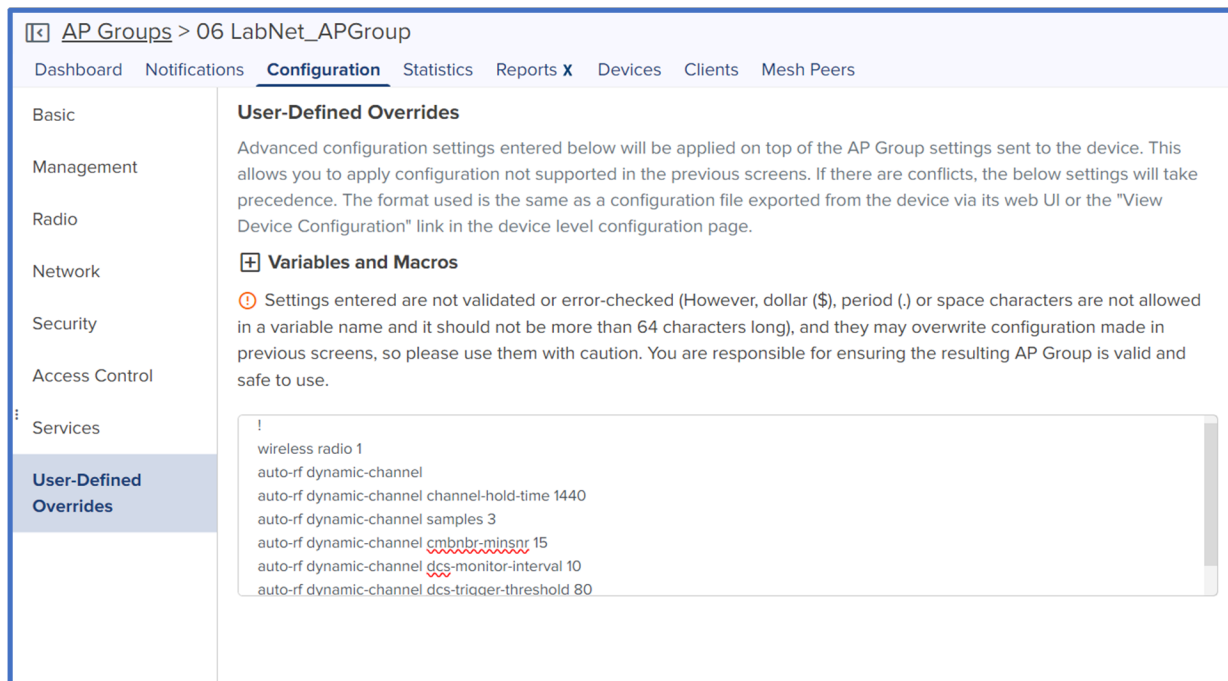
Validation

- Use a site analysis tool such as Ekahau to perform a verification survey.
- Verify coverage and signal strength in all areas.
- Verify that there are not too many 2.4GHz radios (Avoid co-channel interference).
- 20MHz channels only
- Verify signal strength beyond the apartment where the AP is located. How many apartments does the signal bleed into?

User-Defined Overrides

Auto-RF Dynamic Channel - If you are using an older version of cnMaestro, you can enable Auto-RF Dynamic Channel through User-Defined Overrides.

Figure 2: User-Defined Overrides



Copy and paste the below settings:

```
!  
wireless radio 1  
auto-rf dynamic-channel  
auto-rf dynamic-channel channel-hold-time 1440  
auto-rf dynamic-channel samples 3  
auto-rf dynamic-channel cmbnbnr-minsnr 15  
auto-rf dynamic-channel dcs-monitor-interval 10  
auto-rf dynamic-channel dcs-trigger-threshold 80  
auto-rf dynamic-channel channel-bond-threshold 5  
auto-rf dynamic-channel weightage-map-index 1  
auto-rf dynamic-channel congestion-channel-switch on  
auto-rf dynamic-channel congestion-threshold 70  
auto-rf dynamic-channel per-channel-switch on  
auto-rf dynamic-channel acceptance-per-threshold 30  
!
```

```

wireless radio 2
auto-rf dynamic-channel
auto-rf dynamic-channel channel-hold-time 1440
auto-rf dynamic-channel samples 3
auto-rf dynamic-channel cmbnbr-minsnr 15
auto-rf dynamic-channel dcs-monitor-interval 10
auto-rf dynamic-channel dcs-trigger-threshold 80
auto-rf dynamic-channel channel-bond-threshold 5
auto-rf dynamic-channel weightage-map-index 1
auto-rf dynamic-channel congestion-channel-switch on
auto-rf dynamic-channel congestion-threshold 70
auto-rf dynamic-channel per-channel-switch on
auto-rf dynamic-channel acceptance-per-threshold 30
!
wireless radio 3
auto-rf dynamic-channel
auto-rf dynamic-channel channel-hold-time 1440
auto-rf dynamic-channel samples 3
auto-rf dynamic-channel cmbnbr-minsnr 15
auto-rf dynamic-channel dcs-monitor-interval 10
auto-rf dynamic-channel dcs-trigger-threshold 80
auto-rf dynamic-channel channel-bond-threshold 5
auto-rf dynamic-channel weightage-map-index 1
auto-rf dynamic-channel congestion-channel-switch on
auto-rf dynamic-channel congestion-threshold 70
auto-rf dynamic-channel per-channel-switch on
auto-rf dynamic-channel acceptance-per-threshold 30
!

```

1. **Gtk-per-vlan** - Enable **gtk-per-vlan** feature through User-Defined overrides for WLANs which has ePSK security enabled only (not necessary for WLANs that have open/wpa2-psk/802.1x security configured for use without an ePSK).



Note

Double check WLAN number (ie. wlan1, wlan2, etc.) before pushing the configuration.

AP Groups > 06 LabNet_APGroup

Dashboard Notifications **Configuration** Statistics Reports X Devices Clients Mesh Peers

Basic

Management

Radio

Network

Security

Access Control

Services

User-Defined Overrides

User-Defined Overrides

Advanced configuration settings entered below will be applied on top of the AP Group settings sent to the device. This allows you to apply configuration not supported in the previous screens. If there are conflicts, the below settings will take precedence. The format used is the same as a configuration file exported from the device via its web UI or the "View Device Configuration" link in the device level configuration page.

Variables and Macros

ⓘ Settings entered are not validated or error-checked (However, dollar (\$), period (.) or space characters are not allowed in a variable name and it should not be more than 64 characters long), and they may overwrite configuration made in previous screens, so please use them with caution. You are responsible for ensuring the resulting AP Group is valid and safe to use.

```
!
wireless wlan 1
gtk-per-vlan
!
```

Copy and paste the below settings:

```
!
wireless wlan 1
gtk-per-vlan
!
```

Disable minimum rates for management frames

```
!
wireless radio 1
mode gnax
rates management 24
rates min-unicast 6
!
```

```
wireless radio 2
mode default
rates management 24
rates min-unicast 6
```

```
!
wireless radio 3
mode default
rates management 24
rates min-unicast 6
```

```
!
```

General benefits of ePSKs

- ePSK at edge (2000 ePSKs/AP and 50k ePSKs per account)
- Radius auth (Unlimited ePSKs) - 3rd party integration
- Dynamic VLAN (4094 VLANs/Device)
- Authenticating IoT end points (wired and wireless)
- Local/Private Mac Authentication , client can get authenticated since the devices will be identified with the keys.
- When ePSKs are in use, 802.11r is not available

Dynamic VLAN's

Dynamic VLAN assignment separates and isolates devices into different network segments based on the user authorization and their characteristics.

ePSK Creation / Configuration

Adding Single ePSK

- Single User Passphrase
- Create up to 100 users and different passwords for the users
- The username is to easily identify the user
- Specific VLAN to a specific department (Finance/Sales)
- If you don't enter a passphrase, one will be generated for you by cnMaestro.

Figure 3: Add ePSK

Add PSK [X]

Mode
 Single Bulk

User Name *
[Text Input Field]
The number of characters allowed is between 1 and 24

Passphrase
[Text Input Field]
The number of characters allowed is between 8 and 16

MAC Address
[Text Input Field: xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx]

VLAN
[Text Input Field]
VLAN ID should be in between 1 and 4094

[Save]

Adding ePSKs in Bulk

- users are generated for ease of use
- Import and Export options available
- Export the users created and then import back after editing it
- APIs are supported in the On-Premise version and Cloud version
- APIs can be used to generate /delete and view ePSK entries

Figure 4: Adding ePSK in bulk

Add PSK [X]

Mode
 Single Bulk

Count*
[Text Input]
This allows values between 2 and 1024

User Name Prefix*
[Text Input]
Username and Passphrase will be auto generated i.e prefix-1

VLANs
[Text Input]
Use comma ", " separated VLANs. To provide a range use "-".

[Save]

Import/Export and Delete

The Import and Export of ePSK entries is to facilitate exporting the existing ePSK entries as a CSV file and make multiple changes(add/remove) to ePSK data. Once the changes are done, the edited file can be imported back into cnMaestro. Apart from editing the existing file, importing a new batch of user keys, which were generated externally, is also possible. Additionally, deletion of ePSK entries is also possible.



Note

When cloning a WLAN, the ePSKs associated with that WLAN do not transfer with the cloned version. You must export the ePSKs from the original WLAN and import them into the cloned version of the WLAN.

Passphrase Strength

Setting the Passphrase Strength has 3 options,

- Easy - Allows Alphanumeric characters (up to 8 Characters)
- Strong - Allows Alphanumeric and Special Characters (up to 16 Characters)
- Number - Allows Numbers (up to 8 Characters)

API Support

ePSK entries can be generated/deleted and viewed using APIs. This support is available in both on-premises and cloud versions of cnMaestro X.

RADIUS-based Solution - Configuration

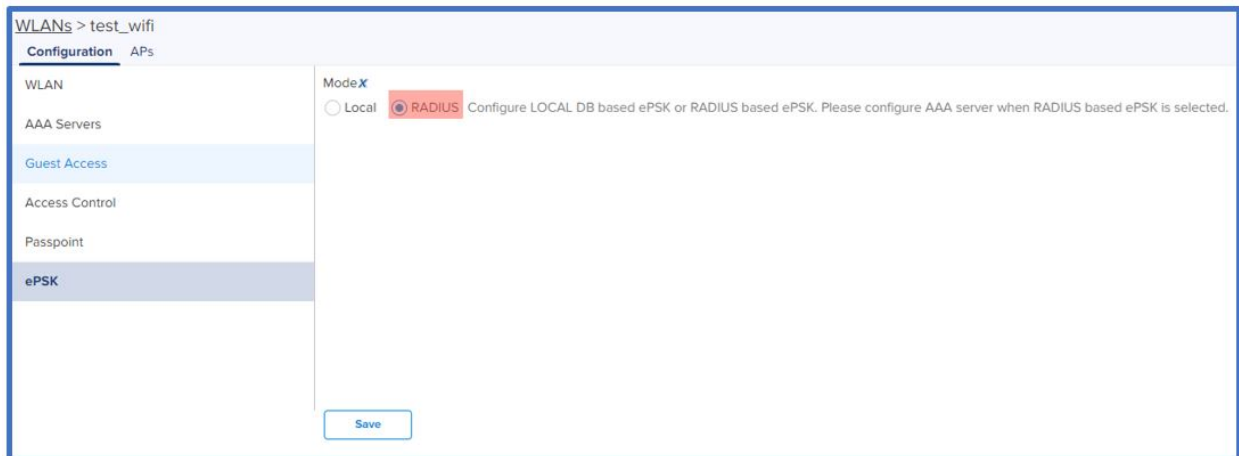
For deployments where it is necessary to create more than 2,000 keys, having the AP-based ePSK solution will be challenging. Since the keys are local on the AP, computing the PMK and authenticating

the users will depend on the AP's resource capability.

RADIUS-based ePSK solution will be a better option for these deployments, where the computation of the PMK will be offloaded to an external AAA server. This allows the solution to scale better.

AAA Vendors already integrated

1. RGNets: <https://www.rgnets.com/>
2. BlueportIQ: <https://www.blueportiq.com/>
3. ElevenOS: <https://www.elevensoftware.com/platform>



The screenshot shows a web-based configuration interface for WLANs. The breadcrumb path is "WLANs > test_wifi". The main menu on the left includes "Configuration" (selected), "APs", "WLAN", "AAA Servers", "Guest Access", "Access Control", "Passpoint", and "ePSK". The "ePSK" section is active, displaying the "ModeX" configuration. Two radio buttons are present: "Local" (unselected) and "RADIUS" (selected). A red box highlights the "RADIUS" option. Below the radio buttons, a note reads: "Configure LOCAL DB based ePSK or RADIUS based ePSK. Please configure AAA server when RADIUS based ePSK is selected." A "Save" button is located at the bottom right of the configuration area.

ePSK Configuration

WLAN Configuration:

1. WLAN Basic and Advanced Configuration

The screenshot shows the 'WLANs > e-PSK' configuration page. The left sidebar lists 'WLAN' as the active section, with other options like 'AAA Servers', 'Guest Access', 'Access Control', 'Passpoint', and 'ePSK'. The main content area is divided into two sections: 'Basic Information' and 'Basic Settings'. 'Basic Information' includes fields for 'Type' (Enterprise WiFi), 'Name' (e-PSK), and 'Description' (e-PSK). 'Basic Settings' includes 'SSID' (ENABLED, SSID: WLAN124), 'Mesh' (Off), 'VLAN' (1), 'Security' (WPA2 Pre-Shared Keys), 'Passphrase' (12345678), 'Radies' (2.4GHz and 5GHz), and 'Client Isolation' (Disable). There are also checkboxes for 'cnMaestro Managed Roaming' and 'Hide SSID'.

2. AAA Configuration

The screenshot shows the 'WLANs > e-PSK' configuration page with the 'AAA Servers' section selected in the sidebar. At the top, there is a checkbox for 'Proxy RADIUS through cnMaestro' with a description: 'Proxy RADIUS packets through cnMaestro (on-premises) instead of directly to the RADIUS server from the AP'. Below this is the 'Authentication Server' section with three rows for configuring hosts, secrets, and ports. The first row has Host: 10.10.10.10, Secret: [masked], and Port: 1812. The second row has Host: [empty], Secret: [masked], and Port: 2049. The third row has Host: [empty], Secret: [masked], and Port: 1812. There are also fields for 'Timeout' (3) and 'Attempts' (1). At the bottom, there are checkboxes for 'Accounting Server' and 'Advanced Settings', and a 'Save' button.

cnMaestro Configuration - Proxy through controller

1. Enable Radius Proxy globally (optional). (This will send all the Radius requests through cnMaestro, so only cnMaestro IP needs to be added as NAS).

This On-Premises instance is not onboarded to cnMaestro Cloud. You can manage this from Administration > Settings > Cloud Connectivity

Administration > Settings

General Notifications Syslog X Webhooks X Cloud Connectivity

PTP
60 GHz cnWave
cnPilot Home (cnPilot R-Series)
Enterprise Wi-Fi (E-Series and XV-Series) and cnPilot Enterprise (ePMP 1000 Hotspot)
cnMatrix
cnVision

Enterprise
Provides a user interface tailored to managing enterprise Wi-Fi deployments consisting of:
Enterprise Wi-Fi (E-Series and XV-Series) and cnPilot Enterprise (ePMP 1000 Hotspot)
cnMatrix

Industrial Internet
Provides a single management system to manage Fixed Wireless, Wi-Fi and IIoT deployments including:
cnRanger
ePMP
PMP
PTP
60 GHz cnWave
cnPilot Home (cnPilot R-Series)
Enterprise Wi-Fi (E-Series and XV-Series) and cnPilot Enterprise (ePMP 1000 Hotspot)
cnReach
cnMatrix
cnVision
Machfu

Advanced Features

WiFiPerf Daemon X Enable to perform Wi-Fi performance test between Wi-Fi AP/CPE and cnMaestro. ⓘ

RADIUS Proxy Enable to configure Proxy RADIUS through cnMaestro feature in WLAN policies.

NAS IP:

Satellite View Enable satellite view in maps. ⓘ

Lock Wi-Fi AP/cnMatrix device Configuration X Enable this option to overwrite any Wi-Fi AP/cnMatrix configuration changes made outside of cnMaestro

2. AAA configuration - Enable Proxy RADIUS through cnMaestro on the WLAN (optional)

WLANs > e-PSK

Configuration APs

WLAN

AAA Servers

Guest Access

Access Control

Passpoint

ePSK

ⓘ Warning: AAA Servers are configured separately for each WLAN.

Proxy RADIUS through cnMaestro
Proxy RADIUS packets through cnMaestro (on-premises) instead of directly to the RADIUS server from the AP

Authentication Server

1. Host Secret Show

2. Host Secret Show

3. Host Secret Show

Timeout Timeout in seconds for each request attempt (1-30)

Attempts Number of attempts before giving up (1-3)

Accounting Server

Advanced Settings

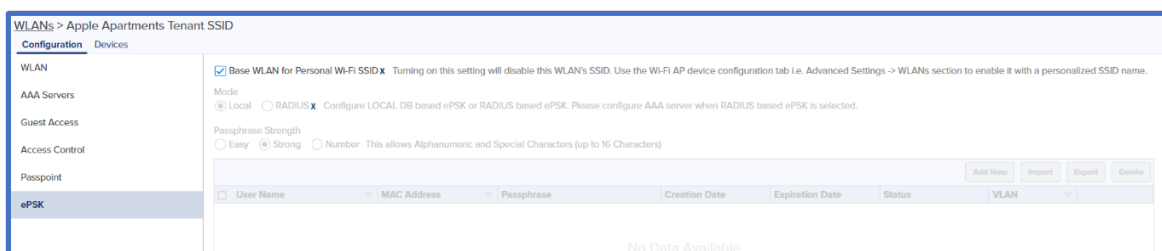
Personal Wi-Fi Network

Benefits of Personal Wi-Fi Network

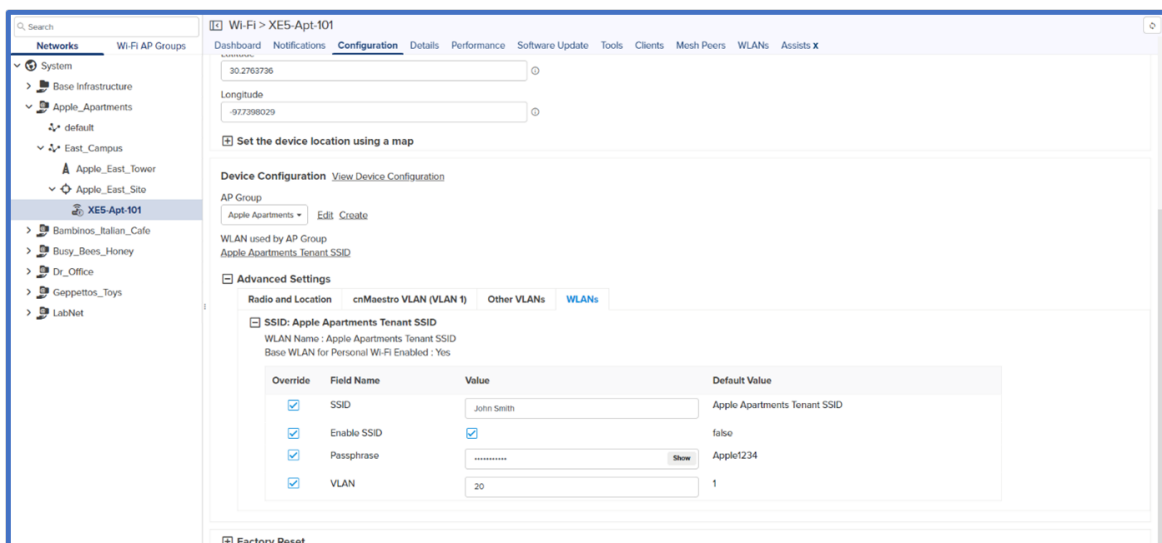
Personal Wi-Fi is a solution designed to address requirements in Multi-Dwelling Units (MDU) and similar hospitality-related networks. Each user on the network effectively operates on their own secure Wi-Fi network, similar to having a personal Wi-Fi router. Users can seamlessly roam across a property with ubiquitous connectivity while maintaining their security via a unique ePSK and unique VLAN. This functionality is provided with a unique SSID for the user in their personal space (apartment, dormitory room, etc.) but with a common property SSID in public areas. Credentials are common across all networks and roaming is seamless to the user. For property managers, this personalized approach ensures tenant privacy and security while minimizing administration overhead

Personal Wi-Fi Network configuration

1. Go to **Configuration > Wi-Fi Profiles > WLANs > WLAN > ePSKs**. At the top of the page, enable **Base WLAN for Personal Wi-Fi SSID**.



2. In the Network Tree, select the AP for the tenant's residence (ie. Apartment 101). Go to the **Configuration > Advanced Settings > WLANs** page and under the SSID: Apple Apartments Production SSID, enable the Overrides for SSID, Enable SSID, Passphrase, and VLAN. Name the SSID something unique to the tenant (ie. John Smith), enable the SSID, and give the SSID a unique password and a unique VLAN. Apply the configuration.



Troubleshooting

- Understand the issues, ask specific questions, and don't assume you know the full scope of the issues
- Review configuration for obvious and immediate improvements
- When possible methodical/ iterative vs "shotgun approach when recommending implementing several changes
- What are the key metrics to track based on the issues
- Start with baselines of the current situation
- Make required changes, collect updated metrics, and compare to the baseline

Show Commands

`show config wireless` - will show the username and ePSK keys on the CLI

`show wireless clients user-group` - will show the username assigned to the client

`service show epsk` - will dump the ePSK logs in the wmd.log file

`service show debug-logs wmd` - to view wmd.log on the CLI

`service debug wmd logging-level debug` - to enable wmd debug level logging

Enable debug logging from AP CLI - to view the ePSK cache entries on the system

```
XV2-2-484686(config)#
```

```
XV2-2-484686(config)# service show epsk
```

```
XV2-2-484686(config)# service debug wmd logging-level debug
```

```
XV2-2-484686(config)# save
```

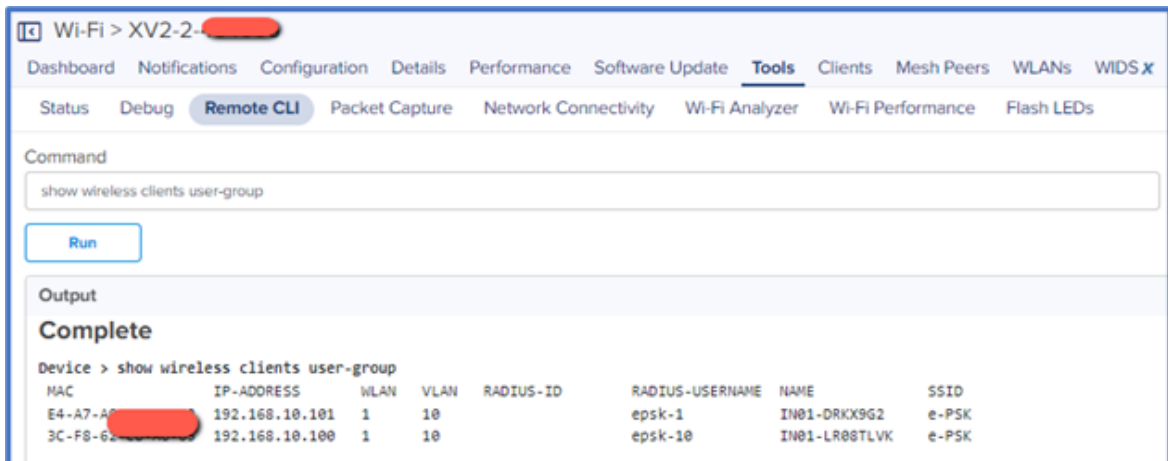
```
[Config Save OK]
```

```
XV2-2-484686(config)#XV2-2-484686(config)# service show debug-logs wmd
```

Remote debugging from cnMaestro

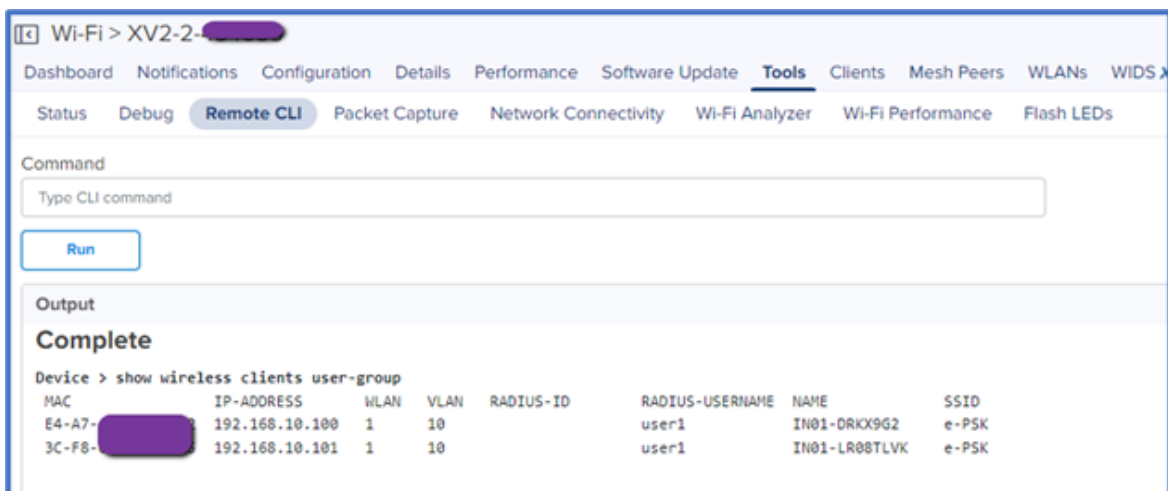
To view the clients connected to the username, run `show wireless clients user-group`

- Individual Keys to connect the wireless station.



RADIUS-USERNAME is different for clients, i.e., clients connected using individual keys.

- Single Key configured to connect multiple wireless clients.



RADIUS-USERNAME is the same for both clients, i.e., clients connected using the same key.

Debugging

Debugging using the cnMaestro dashboard

- Aggregated number of connected clients over time
- Aggregated throughput over time
- Split of 2.4GHz vs 5GHz vs 6GHz connections

Export wireless client data every 6-8 hours.

In Excel, chart Client Connection Duration and SNR

Summary

Residents of multi-dwelling units (MDUs) expect high-performing, secure Wi-Fi with easy access.

Cambium Networks provides high-performance wireless solutions that support MDUs in any configuration or size. This document describes Cambium Networks Enterprise Access Points and cnMaestro management solutions that are best deployed in MDU environments and describes best practices for designing and deploying Wi-Fi networks for optimal results.

Cambium Networks

Cambium Networks delivers wireless communications that work for businesses, communities, and cities worldwide. Millions of our radios are deployed to connect people, places and things with a unified wireless fabric that spans multiple standards and frequencies of fixed wireless and Wi-Fi, all managed centrally via the cloud. Our multi-gigabit wireless fabric offers a compelling value proposition over traditional fiber and alternative wireless solutions. We work with our Cambium certified Connected Partners to deliver purpose built networks for service provider, enterprise, industrial, and government connectivity solutions in urban, suburban, and rural environments, with wireless that just works.

Installation and User Guides	http://www.cambiumnetworks.com/guides
Technical training	https://learning.cambiumnetworks.com/learn
Support website (enquiries)	https://support.cambiumnetworks.com
Main website	http://www.cambiumnetworks.com
Sales enquiries	solutions@cambiumnetworks.com
Warranty	https://www.cambiumnetworks.com/support/standard-warranty/
Telephone number list to contact	http://www.cambiumnetworks.com/contact-us/
Address	Cambium Networks Limited, Unit B2, Linhay Business Park, Eastern Road, Ashburton, Devon, TQ13 7UP United Kingdom



www.cambiumnetworks.com

Cambium Networks and the stylized circular logo are trademarks of Cambium Networks, Ltd. All other trademarks are the property of their respective owners.

© Copyright 2023 Cambium Networks, Ltd. All rights reserved.